CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICSJWG
QUARTERLY NEWSLETTER

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

September 2022

UPCOMING EVENTS

Register Today!

ICSJWG 2022 Fall Virtual Meeting
September 13-14
Agenda and Registration

Trainings:

Quarterly ChemLock Trainings
January 11 & April 12
Course Information -- Jan Registration -- Apr Registration

Industrial Control Systems Evaluation (401v)
Online Virtual Training
September 12-30
Course Information -- Registration

Industrial Control Systems Cybersecurity (301v)
Online Virtual Training
September 19-30
Course Information -- Registration

Industrial Control Systems Cybersecurity (301L)
In-Person Training
October 10-13
Course Information -- Registration

Industrial Control Systems Evaluation (401v)
Online Virtual Training
October 10-28
Course Information -- Registration

Industrial Control Systems Cybersecurity (301v)
Online Virtual Training
October 10-28
Course Information -- Registration

Industrial Control Systems Cybersecurity (301L)
In-Person Training
October 24-27
Course Information -- Registration

Additional ICS Training
CISA Virtual Learning Portal

ICSJWG 2022 Fall Virtual Meeting

The ICSJWG is excited to announce that the registration for the ICSJWG Fall Meeting is open! The meeting will take place virtually on September 13-14, 2022, and will include two full days of presentations, a Capture the Flag activity (see below), technical workshop activities, and a CYBER-Champ© overview. The event will kick off with a keynote by Brandon Wales, Executive Director of CISA, on "Joint Cyber Defense Collaborative – Uniting Cyber Defense."

Registration for the 2022 Fall Virtual Meeting can be found using this link. The registration URL can also be found on our webpage, www.cisa.gov/ICSJWG.

ICSJWG meetings and events are open to all who are interested and are free for attendees.

Capture the Flag

Available as part of the 2022 Fall Virtual Meeting!

A "Capture the Flag" (CTF) activity is available from Saturday, September 10 at 12:00 p.m. ET through Wednesday, September 14 at 12:00 p.m. The CTF is a Jeopardy-style activity with up to five players on each team. During the game, there will be a Mattermost chat server available for players to communicate with each other and CTF administrators. Registration for Capture the Flag will open Thursday, September 8 at 7:00 p.m. ET and remain open until the end of the competition, so players can join at any point.

Register and access Mattermost at www.icsjwgctf.com.

ICSJWG 2023 Spring In-Person Meeting

For the first time since 2019, the ICSJWG will host the Spring Meeting in person. This 3-day event will welcome Industrial Control Systems (ICS) community members from around the globe including those new to the control systems security and critical infrastructure security concepts as well as subject matter experts with years of experience. We look forward to seeing you in person and to continue building our partnership with the ICS Community. Stay tuned for the date and location!

An Introduction to the New National Information Exchange Model (NIEM) Cyber Domain for Cyber Information Sharing

The ICSJWG hosted its latest quarterly webinar on August 10 featuring Ilene Klein from the Cybercrime Support Network. The presentation, *An Introduction to the New National Information Exchange Model (NIEM) Cyber Domain for Cyber Information Sharing*, provided an overview of NIEM and how it can work as a universal translator to increase efficiency and agility, reduce information sharing development efforts, ease long-term maintenance, conserve resources, and promote consistency. Over 165 individuals representing all 16 critical infrastructure sectors attended the webinar which was followed with a lively and in-depth Q&A discussion.

The ICSJWG encourages continued participation in future webinars. If you or a colleague have a topic to be considered for presentation, please reach out to icsjwg.communications@cisa.dhs.gov.

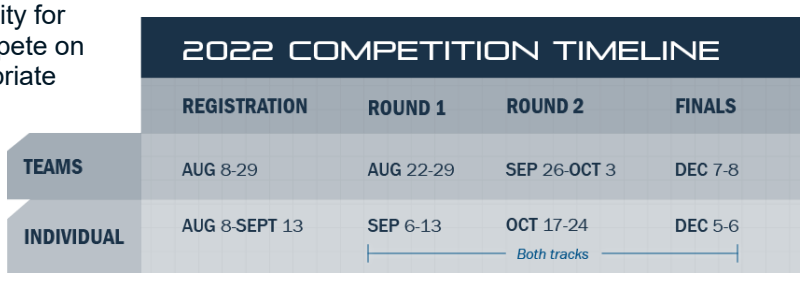
Fourth Annual President's Cup Cybersecurity Competition

Registration closes on September 13!

Don't miss your chance to register for this year's President's Cup. This nationwide competition seeks to identify, recognize, and reward the best cyber talent from across the federal government. Join this year's challenges to take an adventure through space and stretch your abilities through a fun, unique cyber competition.

The President's Cup serves as a training opportunity for the federal cyber workforce. Competitors can compete on their own time to qualify for training or, with appropriate supervisorial approval, during work or duty hours.

Qualifying Round 1 for individuals will start on September 6, 2022 and will run through September 13. Participants will compete in the first two qualifying rounds remotely, and the finals will be held in December at CISA facilities.



The President's Cup is open to federal employees from the executive departments and agencies, including uniformed services. Participant current job function does not need to be focused on cybersecurity. Contractors are not eligible to participate.

Registration for individuals is available at PresidentsCup.cisa.gov until September 13. Don't miss your chance to sign up!

Contributed Content Disclaimer: The advice and instructions provided in the contributed content are specified as is with no warranties and should be confirmed and tested prior to implementation.

Deploying Meaningful Cybersecurity Between Manufacturing SCADA Systems and Programmable Logic Controllers

By: Dennis Lanahan, Vice President for Critical Infrastructure Markets, Owl Cyber Defense

On April 13 of this year, four U.S. federal agencies together issued a joint Cybersecurity Advisory explaining that advanced persistent threat actors have developed tools to fully access certain industrial control systems and supervisory control and data acquisition (SCADA) devices. The agencies include the Department of Energy, CISA, the NSA, and the FBI. This atypical collaboration shows the seriousness and urgency of the threat. It is yet another indicator of the risks currently facing the manufacturing sector of American critical infrastructure where technology may be dated from a time when cyber threats weren't an issue. Companies are now rethinking their manufacturing systems architecture to keep their critical systems safe.

Continue to full article…

ICS4ICS Program Overview

The ISA Global Cybersecurity Alliance has joined forces with CISA and cybersecurity response teams from more than 50 participating companies to adopt FEMA's Incident Command System framework for response structure, roles, and interoperability. This is the system used by First Responders globally when responding to hurricanes, floods, earthquakes, industrial accidents, and other high impact situations. The ICS4ICS program, announced in May 2021, is designed to improve cybersecurity capabilities related to incidents that impact industrial control systems.

Continue to full article…

Ensuring the Security of Industrial Assets

A new open-source standard for security advisories that makes advisories machine readable referred to as "Common Security Advisory Framework" (CSAF) 2.0 has offered help in the form of automation. CSAF 2.0, created by a consortium of companies and organizations including Siemens, Microsoft, Dell, Oracle, Cisco, and the German Federal Office for Information Security (BSI), helps streamline the process of ensuring security advisories are up to date by automatically retrieving advisory updates from manufacturers – a task anyone working on a company's cybersecurity process knows can be arduous. CSAF 2.0 is just the beginning of a new standard for advisories being adopted by companies and organizations.

Continue to full article…

Cyber Secured IACS Reduces the Impact and Assures Safety and Business Continuity

By: Daniel Ehrenreich, Consultant and Lecturer, SCCE

The risk of cyber-attacks against industrial plants is growing at an unprecedented rate. Among the recently published internally and externally generated cyber security incidents, you find attacks that are not directly affecting the industrial process and those which cause operation outage, damage, and supply chain-related attacks. Industrial-type plants controlled by Industrial Automation Control Systems (IACS – an ISA/IEC 62443 standard-related term) must be built with safety, cyber security, and reliability in mind to assure business continuity and prevent damage and protect lives. Different ranges of solutions must be deployed to protect these systems.

This paper explores an innovative approach to Industrial Automation Control Systems (IACS) cyber defense by differentiating between IT and IACS attacks and explaining the types of triads that can serve as cyber defense methods.

Continue to full article…

OT/IoT Security Report – Cyber War Insights, Threats and Trends, Recommendations

With the cyber threat landscape constantly changing, it is more important than ever to understand how it is impacting your organization. In the past six months, we have seen a surge in the frequency and complexity of attacks, as well as the use of new tactics by threat actors. Threats that were once considered unlikely have suddenly become commonplace. Companies that were not previously targeted by ransomware are now finding themselves on the receiving end of these attacks. In addition to this shift, threat actors continue to obfuscate their malicious activity from detection by security solutions.

To strengthen security and minimize future threats, companies need real-time insight into their cyber risk exposure so they can make informed decisions about how best to protect themselves.

Continue to full article...